

05.10.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

REC'D 18 NOV 2004	
WIPO	PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年11月11日

出 願 番 号
Application Number: 特願2003-380849
[ST. 10/C]: [JP 2003-380849]

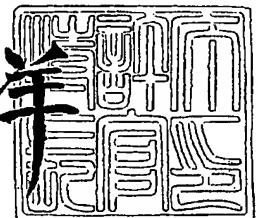
出 願 人
Applicant(s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年11月 5日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 2048150033
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00 640
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 庭野 智
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 徳田 克己
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 三浦 康史
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100109210
 【弁理士】
 【氏名又は名称】 新居 広守
【手数料の表示】
 【予納台帳番号】 049515
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 0213583

【書類名】特許請求の範囲**【請求項 1】**

第 1 の情報提供者の提供する第 1 の情報と、第 2 の情報提供者から提供される前記第 1 の情報と関連する第 2 の情報を利用する端末装置において、

第 3 の情報で指定される情報提供者が署名した前記第 2 の情報を署名検証し利用可否判定する

ことを特徴とする情報利用可否判定方法。

【請求項 2】

前記第 1 の情報が暗号化されている場合に、前記第 3 の情報が前記第 1 の情報の暗号鍵を含むライセンスに格納されている

ことを特徴とする請求項 1 記載の情報利用可否判定方法。

【請求項 3】

前記第 1 の情報が暗号化されている場合に、前記第 3 の情報が暗号化された前記第 1 の情報に格納されている

ことを特徴とする請求項 1 記載の情報利用可否判定方法。

【請求項 4】

前記第 2 の情報が暗号化されている場合に、前記第 3 の情報が暗号化された前記第 2 の情報の暗号鍵を含むライセンスに格納されている

ことを特徴とする請求項 1 記載の情報利用可否判定方法。

【請求項 5】

前記第 3 の情報が、前記第 1 の情報提供者のみと、前記第 1 の情報提供者と前記第 1 の情報提供者が公開鍵証明書に署名した前記第 2 の情報提供者のみと、制限なし、のうちの少なくとも 2 つから 1 つを識別するフラグである

ことを特徴とする請求項 2 ～請求項 4 のいずれか 1 項に記載の情報利用可否判定方法。

【請求項 6】

前記第 3 の情報が、前記第 2 の情報の署名者を一意に特定する識別情報である

ことを特徴とする請求項 2 ～請求項 4 のいずれか 1 項に記載の情報利用可否判定方法。

【請求項 7】

前記端末装置に格納されている前記第 1 の情報提供者の公開鍵証明書を利用することで、前記第 1 の情報提供者が署名したと判断する

ことを特徴とする請求項 5 記載の情報利用可否判定方法。

【請求項 8】

前記端末装置に格納されている前記第 1 の情報提供者を一意に特定する識別情報と前記第 2 の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第 1 の情報提供者が署名したと判断する

ことを特徴とする請求項 5 記載の情報利用可否判定方法。

【請求項 9】

暗号化されている前記第 1 の情報に格納されている前記第 1 の情報提供者を一意に特定する識別情報と前記第 2 の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第 1 の情報提供者が署名したと判断する

ことを特徴とする請求項 5 記載の情報利用可否判定方法。

【請求項 10】

暗号化された前記第 2 の情報の暗号鍵を含む前記第 2 の情報のライセンスに含まれている前記第 1 の情報提供者を一意に特定する識別情報と前記第 2 の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第 1 の情報提供者が署名したと判断する

ことを特徴とする請求項 5 記載の情報利用可否判定方法。

【請求項 11】

前記端末装置で作成する前記第 1 の情報と関連する第 4 の情報に前記端末装置で作成したことを示す識別情報を格納し、前記第 4 の情報に前記端末装置で作成したことを示す識別情報を含む場合、前記第 4 の情報の署名検証を行わない

ことを特徴とする請求項 2 または請求項 3 記載の情報利用可否判定方法。

【請求項 1 2】

前記第 4 の情報の移動範囲指定情報を含む

ことを特徴とする請求項 1 1 記載の情報利用可否判定方法。

【請求項 1 3】

暗号化された前記第 1 の情報に前記第 4 の情報の移動範囲指定情報を含む

ことを特徴とする請求項 1 1 記載の情報利用可否判定方法。

【請求項 1 4】

前記第 2 の情報のライセンスに前記第 4 の情報の移動範囲指定情報を含む

ことを特徴とする請求項 1 1 記載の情報利用可否判定方法。

【請求項 1 5】

前記第 2 の情報に前記第 4 の情報の移動範囲指定情報を含む

ことを特徴とする請求項 1 1 記載の情報利用可否判定方法。

【請求項 1 6】

前記移動範囲指定情報が前記端末装置所有者の所有する前記端末装置に限定する場合に、前記第 4 の情報の少なくとも一部を前記端末装置所有者の所有する前記端末装置に共通の暗号鍵で暗号化する

ことを特徴とする請求項 1 2 ～請求項 1 5 のいずれか 1 項に記載の情報利用可否判定方法。

【請求項 1 7】

前記第 1 の情報のライセンスに前記第 4 の利用可否情報を含む

ことを特徴とする請求項 1 6 記載の情報利用可否判定方法。

【請求項 1 8】

暗号化された前記第 1 の情報に前記第 4 の利用可否情報を含む

ことを特徴とする請求項 1 6 記載の情報利用可否判定方法。

【請求項 1 9】

第 1 の情報提供者の提供する暗号化された第 1 の情報と、第 2 の情報提供者から提供される前記第 1 の情報と関連する第 2 の情報を利用する端末装置において、

前記第 1 の情報の暗号鍵を含むライセンスに前記第 2 の情報を用いて前記第 1 の情報を利用することを指示する参照指示情報を含む

ことを特徴とする情報利用可否判定方法。

【請求項 2 0】

第 1 の情報提供者の提供する暗号化された第 1 の情報と、第 2 の情報提供者から提供される前記第 1 の情報と関連する第 2 の情報を利用する端末装置において、

暗号化された前記第 1 の情報に前記第 2 の情報を用いて前記第 1 の情報を利用することを指示する参照指示情報を含む

ことを特徴とする情報利用可否判定方法。

【請求項 2 1】

前記参照指示情報が前記第 2 の情報を用いるか否かを識別するフラグである

ことを特徴とする請求項 1 9 または請求項 2 0 記載の情報利用可否判定方法。

【請求項 2 2】

前記参照指示情報が前記第 2 の情報を一意に特定する識別情報である

ことを特徴とする請求項 1 9 または請求項 2 0 記載の情報利用可否判定方法。

【請求項 2 3】

前記参照指示情報が前記第 2 の情報の署名者を一意に特定する識別情報である

ことを特徴とする請求項 1 9 または請求項 2 0 記載の情報利用可否判定方法。

【請求項 2 4】

第 1 の情報提供者の提供する暗号化された第 1 の情報と、第 2 の情報提供者から提供される前記第 1 の情報と関連する第 2 の情報を利用する端末装置において、

前記第 1 の情報の暗号鍵を含むライセンスに前記第 2 の情報の編集可否情報を含む

ことを特徴とする情報利用可否判定方法。

【請求項 25】

第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、暗号化された前記第1の情報に前記第2の情報の編集可否情報を含むことを特徴とする情報利用可否判定方法。

【請求項 26】

第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する暗号化された第2の情報を利用する端末装置において、暗号化された前記第2の情報の暗号鍵を含むライセンスに前記第2の情報の編集可否情報を含むことを特徴とする情報利用可否判定方法。

【請求項 27】

第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、前記第2の情報の前記第2の情報の編集可否情報を含むことを特徴とする情報利用可否判定方法。

【請求項 28】

前記編集可否情報が編集可能か否かを識別するフラグである
ことを特徴とする請求項 24～請求項 27のいずれか1項に記載の情報利用可否判定方法。

【請求項 29】

前記編集可否情報が前記第2の情報を一意に特定する識別方法である
ことを特徴とする請求項 24～請求項 27のいずれか1項に記載の情報利用可否判定方法。

【請求項 30】

前記編集可否情報が前記第2の情報の署名者を一意に特定する識別方法である
ことを特徴とする請求項 24～請求項 27のいずれか1項に記載の情報利用可否判定方法。

【請求項 31】

請求項 1 から請求項 30 のいずれか1項に記載の情報利用可否判定方法により、前記第2の情報または前記第4の情報の利用可否を判定する前記端末装置を含むコンテンツ配信システム。

【書類名】明細書

【発明の名称】情報利用可否判定方法およびこの方法を用いたコンテンツ配信システム

【技術分野】

【0001】

本発明は、放送または通信を用いて、映像、音楽などのデジタルコンテンツと、デジタルコンテンツのライセンスと、デジタルコンテンツの属性または制御情報などを含むメタデータを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、メタデータの利用可否判定方法および利用可否判定方法を適用した装置を含むシステムに関する。

【背景技術】

【0002】

デジタルコンテンツを提供するコンテンツプロバイダには、CMスキップのためのシーニンデックスなど意図に反した不正なメタデータの流通を阻止したいという要求があり、メタデータを作成したメタデータプロバイダがメタデータに施すデジタル署名を用いて、不正なメタデータプロバイダを排除する方法が提案されている。

従来、特許文献1などに開示されているように、デジタル署名の検証を用いてメタデータの署名者の正当性とメタデータの中身の改ざんを検出し、メタデータの利用可否を判定している。

【0003】

ここで、従来技術のデジタル署名によるメタデータの利用可否判定について説明する。メタデータのデジタル署名の検証には、デジタル署名されたメタデータと、メタデータ署名者の公開鍵証明書と、CRL (Certificate Revocation List) を用いる。

ここで、メタデータへのデジタル署名は、コンテンツプロバイダ、または、メタデータプロバイダが行う。端末装置では、メタデータを利用する場合、次の手順でメタデータの利用可否判定を行う。

【0004】

まず、メタデータにデジタル署名した署名者の署名者IDがCRLに含まれているか確認する。ここで、署名者IDとは、署名者を一意に特定する識別情報である。

署名者IDがCRLに含まれている場合は、メタデータが利用不可と判定する。

署名者IDがCRLに含まれていない場合は、メタデータの署名を公開鍵証明書で検証し改ざん検出する。

【0005】

改ざんが検出された場合は、メタデータが利用不可と判定する。

改ざんが検出されない場合は、メタデータが利用可能と判定する。

以上、従来技術のデジタル署名によるメタデータの利用可否判定について概略を説明した。

尚、デジタル署名の検証については、非特許文献1が詳しい。

【特許文献1】特開2001-239148号公報

【非特許文献1】ウォーウィック・フォード+マイケル・バウム著「デジタル署名と暗号技術」 株式会社ピアソン・エデュケーション 1997年

【発明の開示】

【発明が解決しようとする課題】

【0006】

デジタル署名の検証によるメタデータの利用可否判定では、少なくとも1回は不正なメタデータによる障害が発生し、不正発見後にCRLを作成する。このため、万が一にも不正なメタデータによる障害が発生しては困る重要なコンテンツでは、コンテンツプロバイダは、自身がメタデータの中身を確認しデジタル署名したメタデータのみ利用を許可したいという要求がある。この場合、従来のデジタル署名の検証だけでは要求を実現できないという課題がある。

【0007】

また、ユーザはメタデータを私的に作成しユーザの所有する端末装置のみで利用したいが、従来のデジタル署名によるメタデータの利用可否判定では、全ての端末装置で利用可能にするか利用不可能にするかしかできない。このため、ユーザの作成したメタデータの利用範囲をユーザの所有する端末装置だけに限定できないという課題がある。

また、コンテンツプロバイダは、コンテンツによっては、ユーザによるメタデータの作成や編集を制限したい場合や、コンテンツプロバイダが指定したメタデータを利用させたい場合があるが、デジタル署名だけでは実現できないという課題がある。

【0008】

本発明は、こうした従来の問題点を解決するものであり、コンテンツ配信システムにおいて、コンテンツプロバイダが、コンテンツ毎に、利用可能なメタデータを限定し、ユーザが作成したメタデータの利用範囲を限定することを可能とするメタデータ利用可否判定方法とメタデータ利用可否判定方法による判定を行う端末装置を含むコンテンツ配信システムを提供することを目的としている。

【課題を解決するための手段】

【0009】

本発明の請求項1記載の情報利用可否判定方法は、第1の情報提供者の提供する第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、第3の情報で指定される情報提供者が署名した前記第2の情報を署名検証し利用可否判定することを特徴としている。

本発明の請求項2記載の情報利用可否判定方法は、請求項1記載の情報利用可否判定方法であって、前記第1の情報が暗号化されている場合に、前記第3の情報が前記第1の情報の暗号鍵を含むライセンスに格納されていることを特徴としている。

【0010】

本発明の請求項3記載の情報利用可否判定方法は、請求項1記載の情報利用可否判定方法であって、前記第1の情報が暗号化されている場合に、前記第3の情報が暗号化された前記第1の情報の情報に格納されていることを特徴としている。

本発明の請求項4記載の情報利用可否判定方法は、請求項1記載の情報利用可否判定方法であって、前記第2の情報が暗号化されている場合に、前記第3の情報が暗号化された前記第2の情報の暗号鍵を含むライセンスに格納されていることを特徴としている。

【0011】

本発明の請求項5記載の情報利用可否判定方法は、請求項2～請求項4のいずれか1項に記載の情報利用可否判定方法であって、前記第3の情報が、前記第1の情報提供者のみと、前記第1の情報提供者と前記第1の情報提供者が公開鍵証明書に署名した前記第2の情報提供者のみと、制限なし、のうちの少なくとも2つから1つを識別するフラグであることを特徴としている。

【0012】

本発明の請求項6記載の情報利用可否判定方法は、請求項2～請求項4のいずれか1項に記載の情報利用可否判定方法であって、前記第3の情報が、前記第2の情報の署名者を一意に特定する識別情報であることを特徴としている。

本発明の請求項7記載の情報利用可否判定方法は、請求項5記載の情報利用可否判定方法であって、前記端末装置に格納されている前記第1の情報提供者の公開鍵証明書を利用することで、前記第1の情報提供者が署名したと判断することを特徴としている。

【0013】

本発明の請求項8記載の情報利用可否判定方法は、請求項5記載の情報利用可否判定方法であって、前記端末装置に格納されている前記第1の情報提供者を一意に特定する識別情報と前記第2の情報の含まれる署名者を一意に特定する識別情報が一致することで、前記第1の情報提供者が署名したと判断することを特徴としている。

本発明の請求項9記載の情報利用可否判定方法は、請求項5記載の情報利用可否判定方法であって、暗号化されている前記第1の情報の情報に格納されている前記第1の情報提供者を

一意に特定する識別情報と前記第2の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第1の情報提供者が署名したと判断することを特徴としている。

【0014】

本発明の請求項10記載の情報利用可否判定方法は、請求項5記載の情報利用可否判定方法であって、暗号化された前記第2の情報の暗号鍵を含む前記第2の情報のライセンスに含まれている前記第1の情報提供者を一意に特定する識別情報と前記第2の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第1の情報提供者が署名したと判断することを特徴としている。

【0015】

本発明の請求項11記載の情報利用可否判定方法は、請求項2または請求項3記載の情報利用可否判定方法であって、前記端末装置で作成する前記第1の情報と関連する第4の情報に前記端末装置で作成したことを示す識別情報を格納し、前記第4の情報に前記端末装置で作成したことを示す識別情報を含む場合、前記第4の情報の署名検証を行わないことを特徴としている。

【0016】

本発明の請求項12記載の情報利用可否判定方法は、請求項11記載の情報利用可否判定方法であって、前記第4の情報の移動範囲指定情報を含むことを特徴としている。

本発明の請求項13記載の情報利用可否判定方法は、請求項11記載の情報利用可否判定方法であって、暗号化された前記第1の情報に前記第4の情報の移動範囲指定情報を含むことを特徴としている。

【0017】

本発明の請求項14記載の情報利用可否判定方法は、請求項11記載の情報利用可否判定方法であって、前記第2の情報のライセンスに前記第4の情報の移動範囲指定情報を含むことを特徴としている。

本発明の請求項15記載の情報利用可否判定方法は、請求項11記載の情報利用可否判定方法であって、前記第2の情報に前記第4の情報の移動範囲指定情報を含むことを特徴としている。

【0018】

本発明の請求項16記載の情報利用可否判定方法は、請求項12～請求項15のいずれか1項に記載の情報利用可否判定方法であって、前記移動範囲指定情報が前記端末装置所有者の所有する前記端末装置に限定する場合に、前記第4の情報の少なくとも一部を前記端末装置所有者の所有する前記端末装置に共通の暗号鍵で暗号化することを特徴としている。

【0019】

本発明の請求項17記載の情報利用可否判定方法は、請求項16記載の情報利用可否判定方法であって、前記第1の情報のライセンスに前記第4の利用可否情報を含むことを特徴としている。

本発明の請求項18記載の情報利用可否判定方法は、請求項16記載の情報利用可否判定方法であって、暗号化された前記第1の情報に前記第4の利用可否情報を含むことを特徴としている。

【0020】

本発明の請求項19記載の情報利用可否判定方法は、第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、前記第1の情報の暗号鍵を含むライセンスに前記第2の情報をういて前記第1の情報を利用することを指示する参照指示情報を含むことを特徴としている。

【0021】

本発明の請求項20記載の情報利用可否判定方法は、第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、暗号化された前記第1の情報に前記第2の情報を

いて前記第1の情報を利用することを指示する参照指示情報を含むことを特徴としている。

【0022】

本発明の請求項21記載の情報利用可否判定方法は、請求項19または請求項20記載の情報利用可否判定方法であって、前記参照指示情報が前記第2の情報を有するか否かを識別するフラグであることを特徴としている。

本発明の請求項22記載の情報利用可否判定方法は、請求項19または請求項20記載の情報利用可否判定方法であって、前記参照指示情報が前記第2の情報を一意に特定する識別情報であることを特徴としている。

【0023】

本発明の請求項23記載の情報利用可否判定方法は、請求項19または請求項20記載の情報利用可否判定方法であって、前記参照指示情報が前記第2の情報の署名者を一意に特定する識別情報であることを特徴としている。

本発明の請求項24記載の情報利用可否判定方法は、第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、前記第1の情報の暗号鍵を含むライセンスに前記第2の情報の編集可否情報を含むことを特徴としている。

【0024】

本発明の請求項25記載の情報利用可否判定方法は、第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、暗号化された前記第1の情報の前記第2の情報の編集可否情報を含むことを特徴としている。

本発明の請求項26記載の情報利用可否判定方法は、第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する暗号化された第2の情報を利用する端末装置において、暗号化された前記第2の情報の暗号鍵を含むライセンスに前記第2の情報の編集可否情報を含むことを特徴としている。

【0025】

本発明の請求項27記載の情報利用可否判定方法は、第1の情報提供者の提供する暗号化された第1の情報と、第2の情報提供者から提供される前記第1の情報と関連する第2の情報を利用する端末装置において、前記第2の情報の前記第2の情報の編集可否情報を含むことを特徴としている。

本発明の請求項28記載の情報利用可否判定方法は、請求項24～請求項27のいずれか1項に記載の情報利用可否判定方法であって、前記編集可否情報が編集可能か否かを識別するフラグであることとしている。

【0026】

本発明の請求項29記載の情報利用可否判定方法は、請求項24～請求項27のいずれか1項に記載の情報利用可否判定方法であって、前記編集可否情報が前記第2の情報を一意に特定する識別方法であることを特徴としている。

本発明の請求項30記載の情報利用可否判定方法は、請求項24～請求項27のいずれか1項に記載の情報利用可否判定方法であって、前記編集可否情報が前記第2の情報の署名者を一意に特定する識別方法であることを特徴としている。

【0027】

本発明の請求項31記載のコンテンツ配信システムは、請求項1～請求項30のいずれか1項に記載の情報利用可否判定方法により、前記第2の情報または前記第4の情報の利用可否を判定する前記端末装置を含むことを特徴としている。

【発明の効果】

【0028】

本発明によれば、CRLを用いずに、コンテンツのライセンスにより、利用可能なメタデータをコンテンツプロバイダがデジタル署名したメタデータのみに限定することが可能となる。また、コンテンツプロバイダが指定したメタデータを利用させることが可能とな

る。

さらに、ユーザによるメタデータの作成、および編集を制限することや、ユーザが作成したメタデータの移動範囲を制限することが可能となる。

【発明を実施するための最良の形態】

【0029】

以下、本発明における実施の形態について、図面を用いて詳細に説明する。

図1は、本発明における実施の形態に関わるコンテンツ配信システム1の全体の概略構成を示す図である。図1に示すように、コンテンツ配信システムは、ライセンス管理サーバ100と、会員管理サーバ200と、コンテンツプロバイダ300と、メタデータプロバイダ400と、CA500と、端末装置600とを備え、伝送路Nで接続されている。

【0030】

ライセンス管理サーバ100は、少なくとも、暗号化コンテンツ310のライセンス110の作成と、ライセンス110の端末装置600への送信を行う。

会員管理サーバ200は、少なくとも、ユーザ情報DB210を管理し、端末装置600にドメイン鍵212を送信する。

コンテンツプロバイダ300は、コンテンツ提供者側に設置される装置であって、少なくとも、暗号化コンテンツ310の作成と、暗号化コンテンツ310の端末装置600への送信を行う。

【0031】

メタデータプロバイダ400は、コンテンツに対するメタデータを作成する作成者側に設定される装置であって、少なくとも、メタデータ410の作成と、メタデータ410の端末装置600への送信を行う。

CA500は、公開鍵証明書などを作成する作成者側に設置される装置であって、少なくとも、公開鍵証明書510の作成と、CRL520の作成と、CRL520の端末装置600への送信を行う。

【0032】

端末装置600は、少なくとも、暗号化コンテンツ310と、メタデータ410の利用を行う。尚、端末装置600には耐タンパ部があり、認証通信や暗号鍵の取得や暗号化や復号などの暗号が関連する処理は、暗号鍵の流出などが発生しないように耐タンパ部で行われる。

伝送路Nは、インターネット等の通信ネットワークや、デジタル放送、あるいは、これらが複合したネットワークである。

【0033】

次に、コンテンツ配信システム1の各構成要素が保有するデータについて説明する。

(1) ライセンス110

ライセンス管理サーバ100は、図2に示すライセンス110を保有し、端末装置600に送信する。ライセンス110は、ライセンスID111と、コンテンツID112と、コンテンツプロバイダID113と、利用条件114と、コンテンツ暗号鍵115から構成されている。

【0034】

ライセンスID111は、ライセンス管理サーバ100でのライセンス110の識別に用いる。コンテンツID112は、ライセンス110と暗号化コンテンツ310を対応付けるために用いる。コンテンツプロバイダID113は、ライセンス110で制御されるコンテンツのコンテンツプロバイダの識別に用いる。利用条件114は、コンテンツの利用制御に用いる。利用条件114は、例えば、“3回利用可能”などの情報である。コンテンツ暗号鍵115はコンテンツの復号に用いる。

【0035】

(2) ユーザ情報DB210

会員管理サーバ200は、図3に示すユーザ情報DB210を保有し、端末装置600からの端末登録要求に応じて、ドメイン鍵212を送信する。ユーザ情報DB210は、

ユーザID 211と、ドメイン鍵 212の組から構成される。

ユーザID 211とは、端末装置 600の所有者毎に与えられるIDである。

【0036】

ドメインとはユーザの所有する端末装置 600で構成される集合であり、ドメイン鍵 212とは、同じドメイン鍵 212を持つ端末装置間のみにデータの送受信が限定されるように、データの暗号化や、認証通信に用いる暗号鍵のことである。

例えば、図3において、「XXXAAA」のユーザID 211に対して、「XXXCCC」のドメイン鍵 212が割り当てられていることを示している。

【0037】

(3) 暗号化コンテンツ 310

コンテンツプロバイダ (CP) 300は、コンテンツプロバイダID 113と、コンテンツプロバイダの秘密鍵と、当該秘密鍵に対する公開鍵と、公開鍵証明書と、コンテンツ暗号鍵 115と、図4に示す暗号化コンテンツ 310を保有する。

暗号化コンテンツ 310はコンテンツID 311と、コンテンツプロバイダID 312と、コンテンツ本体 313から構成され、ライセンス 110のコンテンツ暗号鍵 115でコンテンツプロバイダID 312とコンテンツ本体 313が暗号化されている。

【0038】

コンテンツID 311は、ライセンス 110と暗号化コンテンツ 310を対応付けるために用いる。コンテンツプロバイダID 312は、暗号化コンテンツ 310の提供者を識別するために用いる。コンテンツ本体 313は、映像または音楽などのデジタルデータである。

【0039】

(4) メタデータ 410

メタデータプロバイダ 400は、メタデータプロバイダIDと、メタデータプロバイダの秘密鍵と、当該秘密鍵に対する公開鍵と、公開鍵証明書 510と、図5に示すメタデータ 410を保有する。

【0040】

メタデータ 410は、メタデータ本体 411と、メタデータ署名者ID 412と、デジタル署名 413とから構成されている。メタデータ本体 411にはメタデータを識別するためのメタデータIDと、コンテンツIDなどの属性情報と、コンテンツの位置情報と、シーンインデックスなどのコンテンツの制御情報などが含まれる。メタデータ署名者ID 412は、メタデータ 410にデジタル署名した署名者を識別するために用いる。デジタル署名 413は、メタデータ本体 411の改ざん検出に用いる。

【0041】

(5) CRL 520

CA (Certification Authority) 500は、図7に示すCRL 520と、CAの秘密鍵と、公開鍵を保有する。

CRL 520は、少なくとも、更新日時 521とリボークされた主体者ID 522から構成されている。リボークとは、主体者ID 522で特定される署名者によるデジタル署名を無効化することである。更新日時 521は、例えば、CRL 520を作成した日付であり、CRL 520のバージョン確認に用いる。リボークされた主体者ID 522は、無効化する署名者の識別に用いる。

【0042】

(6) 公開鍵証明書 510

また、コンテンツプロバイダ 300およびメタデータプロバイダ 400が主体者として図6に示す公開鍵証明書 510の作成を依頼した時、主体者公開鍵 512と引き換えに公開鍵証明書 510を主体者に送信する。

公開鍵証明書 510は、少なくとも、主体者ID 511と、主体者公開鍵 512と、デジタル署名 513と、証明書署名者ID 514から構成されている。

【0043】

尚、主体者ID511は公開鍵証明書510の主体者を識別するIDであり、例えば、X.509の証明書におけるシリアル番号を用いてもよい。主体者公開鍵512は、主体者ID511で特定される署名者のデジタル署名の検証に用いる。デジタル署名513は、少なくとも、主体者ID511と、主体者公開鍵512の改ざん検出に用いる。証明書署名者ID514は、公開鍵証明書510にデジタル署名した署名者の特定に用いる。

【0044】

コンテンツ配信システム1におけるメタデータ410とコンテンツ利用処理概略は、例えば、図10に示す手順で行われる。

以降にコンテンツ配信システム1の各構成要素の処理について説明する。

端末装置600は、会員管理サーバ200からドメイン鍵212を取得（ステップS1000）し、コンテンツプロバイダ300から暗号化コンテンツ310を受信（ステップS1010）し、ライセンス管理サーバ100からライセンス110を受信（ステップS1020）し、メタデータプロバイダ400からメタデータ410を受信（ステップS1030）し、メタデータ410とコンテンツを利用（ステップS1040）する。

【0045】

会員管理サーバ200は、端末装置600にドメイン鍵212を配信（ステップS1100）する。

コンテンツプロバイダ300は、暗号化コンテンツ310を作成（ステップS1200）し、端末装置600に暗号化コンテンツ310を送信（ステップS1210）する。

ライセンス管理サーバ100は、ライセンス110を作成（ステップS1300）し、端末装置600にライセンス110を送信（ステップS1310）する。

【0046】

メタデータプロバイダ400は、メタデータ410を作成（ステップS1400）し、端末装置600にメタデータ410を送信（ステップS1410）する。

図示しないが、CA500は、コンテンツプロバイダ300と、メタデータプロバイダ400から公開鍵証明書510の要求がある都度、公開鍵証明書510を作成して、要求したコンテンツプロバイダ300と、メタデータプロバイダ400に送信し、コンテンツプロバイダ300からメタデータプロバイダ400のリボーク要求がある都度、CRLを作成して端末装置600に送信する。

【0047】

尚、以下の説明に記述されるコンテンツの暗号化方式は、AES (Advanced Encryption Standard) や Triple DES (Data Encryption Standard) 等の共通鍵暗号アルゴリズムが、デジタル署名の方式には、RSA や ECDSA (Elliptic Curve Digital Signature Algorithm) 等の公開鍵暗号アルゴリズムが用いられるのが一般的であり、以下に説明する処理は特定の暗号方式に依存しない。また、ハッシュ計算方式は、SHA-1 (Secure Hash Algorithm 1) や MD5 等が用いられるのが一般的であり、以下に説明する処理は特定のハッシュ計算方式に依存しない。

【0048】

また、ライセンス管理サーバ100と、会員管理サーバ200と、コンテンツプロバイダ300とメタデータプロバイダ400とから端末装置600に送信されるコンテンツ選択画面等のユーザインタフェース画面は、インターネットを通じて、HTTP等のプロトコルにより送信される、HTML (HyperText Markup Language) や XML (Extensible Markup Language) 等のスクリプト言語で記述されたウェブページ、あるいは、デジタル放送により送信される、BML (Broadcasting Markup Language) で記述されたページが一般的であり、以下に説明する処理は特定のページ記述方式に依存しない。

【0049】

会員管理サーバ200の処理について説明する。

(ドメイン鍵送信S1100)

会員管理サーバ200は、端末装置600からのユーザID211を含む端末登録要求を受信し、ユーザ情報DB210から対応するドメイン鍵212を取得し送信する。尚、ユーザ情報DB210にはユーザID211とドメイン鍵212があらかじめ登録されている。

コンテンツプロバイダ300の処理について説明する。

【0050】

(暗号化コンテンツ作成S1200)

コンテンツプロバイダ300は、コンテンツ本体313に対して、コンテンツ毎に異なるコンテンツID311と、コンテンツプロバイダ毎に異なるコンテンツプロバイダID312をつけて、コンテンツプロバイダID312とコンテンツ本体313をコンテンツ暗号鍵115で暗号化して暗号化コンテンツ310を作成する。

【0051】

(暗号化コンテンツ送信S1210)

コンテンツプロバイダ300は、端末装置600のコンテンツ選択要求に応じて、コンテンツ選択画面を作成し、端末装置600へ送信する。コンテンツ選択画面は端末装置600がコンテンツを選択すると対応するコンテンツID311を含むコンテンツ取得要求がコンテンツプロバイダ300に送信されるようになっており、コンテンツプロバイダ300はコンテンツ取得要求に含まれるコンテンツID311に対応した暗号化コンテンツ310を端末装置600に送信する。尚、コンテンツプロバイダ300から端末装置600への暗号化コンテンツ310の送信は、ストリーミングでもファイル配信でもよい。

ライセンス管理サーバ100の処理について説明する。

【0052】

(ライセンス作成S1300)

ライセンス管理サーバ100は、コンテンツプロバイダ300からコンテンツID112とコンテンツプロバイダID113と利用条件114とコンテンツ暗号鍵115を受信し、ライセンスID111をつけてライセンス110を作成する。利用条件114には、コンテンツの利用制御とメタデータ410の利用制御に関する情報が含まれている。

【0053】

コンテンツの利用制御に関する情報としては、利用有効期限情報と、利用可能回数情報などがある。

利用有効期限情報としては、例えば、“2005年12月31日まで利用可能”などの情報が含まれる。

利用可能回数情報としては、例えば、“3回利用可能”などの情報が含まれる。

【0054】

メタデータの利用制御に関する情報としては、メタデータの署名者識別情報と、メタデータの参照指示情報と、メタデータの編集可否情報と、ユーザ作成メタデータによる制御可否情報と、ユーザ作成メタデータの移動範囲指定情報などがある。

メタデータの署名者識別情報としては、例えば、メタデータの署名者として、“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”などの署名者識別情報が含まれる。ここで、コンテンツプロバイダに委任されたメタデータプロバイダとは、コンテンツプロバイダ300がデジタル署名した公開鍵証明書510を持つメタデータプロバイダ400のことであり、それ以外のメタデータプロバイダ400よりもコンテンツプロバイダ300にとっての信頼性は高い。

【0055】

尚、メタデータの署名者識別情報は、利用を許可または不許可するメタデータ署名者ID412でもよい。

メタデータの参照指示情報としては、例えば、暗号化コンテンツ310とともに配信するメタデータ410の参照を強制したい場合には、メタデータ参照指示フラグが含まれる

。尚、参照指示情報はメタデータ参照指示フラグ、あるいは、参照を強制させたいメタデータのID、あるいは、メタデータの署名者IDのいずれでもよい。尚、本実施の形態では、コンテンツのライセンスにメタデータの参照指示情報を含む例について記述するが、暗号化コンテンツ310に参照指示情報を含む場合でもよい。

【0056】

メタデータの編集可否情報としては、例えば、“メタデータ編集可能”または“メタデータ編集不可”を示すフラグ、あるいは、編集可能なまたは編集不可能なメタデータのID、あるいは、編集可能なまたは編集不可能なメタデータデジタル署名のメタデータ署名者ID412のいずれでもよい。尚、本実施の形態では、メタデータの編集可否情報がコンテンツのライセンスに含まれる場合について記述するが、暗号化コンテンツ310に含まれる場合、あるいは、メタデータ410のメタデータ本体411に含まれる場合、あるいは、コンテンツと同様にメタデータ410が暗号化され、暗号鍵を含むメタデータ410のライセンスがある場合、メタデータ410のライセンスに含まれる場合のいずれでもよい。

【0057】

ユーザ作成メタデータによる制御可否情報としては、例えば、“ユーザ作成メタデータによる制御可能”または“ユーザ作成メタデータによる制御不可”を示すフラグなどの情報が含まれる。尚、本実施の形態では、ユーザ作成メタデータによる制御可否情報がコンテンツのライセンスに含まれる場合について記述するが、暗号化コンテンツ310に含まれる場合でもよい。

【0058】

ユーザ作成メタデータの移動範囲指定情報としては、例えば、“移動無制限”または“メタデータを作成したユーザが所有する端末装置に限定”などの移動可能範囲を示す情報が含まれる。尚、本実施の形態では、ユーザ作成メタデータの移動範囲指定情報がコンテンツのライセンスに含まれる場合について記述するが、暗号化コンテンツ310に含まれる場合、あるいは、メタデータ410のメタデータ本体411に含まれる場合、あるいは、コンテンツと同様にメタデータが暗号化され、暗号鍵を含むメタデータのライセンスがある場合、メタデータのライセンスに含まれる場合のいずれでもよい。

【0059】

(ライセンス送信S1310)

ライセンス管理サーバ100は、端末装置600からのライセンス取得要求に応じてライセンスの購入処理を行った後、端末装置600にライセンス110を送信する。尚、ライセンスの購入処理は図示しない購入サーバとライセンス管理サーバ100との間で行われる。

【0060】

メタデータプロバイダ400の処理について説明する。

(メタデータ作成S1400)

メタデータプロバイダ400は、メタデータ本体411を作成し、署名者412にメタデータプロバイダのIDを格納し、メタデータ本体411とメタデータ署名者ID412に対するデジタル署名413を作成する。メタデータ410のデジタル署名をコンテンツプロバイダ300が行う場合もあり、その場合には、メタデータプロバイダ400からコンテンツプロバイダ300にメタデータ本体411を送信し、コンテンツプロバイダ300が、メタデータ署名者ID412にコンテンツプロバイダのIDを格納し、コンテンツプロバイダのデジタル署名413を作成してメタデータ410を作成し、メタデータプロバイダ400に送信する。

【0061】

(メタデータ送信S1410)

メタデータプロバイダ400は、端末装置600からのメタデータ取得要求に応じて、メタデータ選択画面を作成し、端末装置600に送信する。メタデータ選択画面は端末装置600がメタデータを選択すると対応するメタデータIDを含むメタデータ取得要求がメ

タデータプロバイダ400に送信されるようになっており、メタデータプロバイダ400はメタデータ取得要求に含まれるメタデータIDに対応したメタデータ410を端末装置600に送信する。

CA500の処理について説明する。

【0062】

(公開鍵証明書作成)

CA500は、コンテンツプロバイダ300またはメタデータプロバイダ400から主体者公開鍵512を含む公開鍵証明書510の作成要求を受信し、主体者公開鍵512毎に異なる主体者ID511を生成し、主体者ID511と主体者公開鍵512に対するデジタル署名513を作成し、主体者ID511と、主体者公開鍵512と、デジタル署名513とから構成される公開鍵証明書510を作成しコンテンツプロバイダ300またはメタデータプロバイダ400に送信する。

【0063】

尚、コンテンツプロバイダ300が、信頼するメタデータプロバイダ400にメタデータのデジタル署名を委任する場合などに、コンテンツプロバイダ300が、メタデータプロバイダ400の公開鍵証明書510の作成処理を行うことがある。この場合、コンテンツプロバイダ300がデジタル署名した公開鍵証明書510を持つメタデータプロバイダ400は、それ以外のメタデータプロバイダ400よりもコンテンツプロバイダ300に信頼されていると判断する場合もある。このような方法は、証明書パスと呼ばれる一般的な方法で、非特許文献1が詳しい。

【0064】

(CRL作成)

CA500は、コンテンツプロバイダ300からリボーク対象のメタデータプロバイダ400のIDを含むCRL更新要求を受信し、更新日時521を、例えば、“2003年1月1日”から“2003年11月11日”のように、CRL作成日時に更新し、受信したメタデータプロバイダ400のIDを主体者ID522に追加し、CRL520を作成し端末装置600に送信する。

端末装置600の処置について説明する。

【0065】

(ドメイン鍵受信S1000)

まず、端末装置600のドメイン鍵受信処理について説明する。

端末装置600は、会員管理サーバ200に会員登録要求を送信し、ドメイン鍵212を受信する。ドメイン鍵212は端末装置600に格納される。通信路Nを通じて、会員管理サーバ200と端末装置600との間でドメイン鍵212を送受信する場合には、セキュリティを確保するため、SSL(Secure Socket Layer)などの安全な認証チャネル(Secure Authenticated Channel、以下、SACと記述)を確立してから、データの送受信を行う。端末装置600は、受信したライセンス110を端末装置600に格納する。尚、本実施の形態では、会員管理サーバ200と端末装置600との間でSACを確立してからドメイン鍵212を送受信したが、端末装置600に固有鍵が格納されており、会員管理サーバ200が各端末装置600の固有鍵を管理している場合には、ドメイン鍵212を端末装置600の固有鍵で暗号化して会員管理サーバ200から端末装置600に送信するなどしてもよい。

【0066】

(暗号化コンテンツ受信S1010)

次に、暗号化コンテンツ310の受信処理について説明する。

端末装置600は、コンテンツプロバイダ300に、コンテンツ選択要求を送信し、コンテンツ選択画面を受信する。端末装置600は受信したコンテンツ選択画面を表示し、ユーザの操作により選択されたコンテンツのコンテンツID311を含むコンテンツ取得要求をコンテンツプロバイダ300に送信し、コンテンツプロバイダ300から暗号化コンテンツ310を受信する。尚、コンテンツプロバイダ300から端末装置600への暗

号化コンテンツ 310 の送信は、ストリーミングでもファイル配信でもよい。

【0067】

(ライセンス受信 S1020)

次に、コンテンツのライセンス 110 の受信処理について説明する。

端末装置 600 は、ライセンス管理サーバ 100 に、ライセンス選択要求を送信し、ライセンス選択画面を受信する。端末装置 600 は受信したライセンス選択画面を表示し、端末装置 600 は、ユーザの操作により選択されたライセンス 110 のライセンス 111 ID を含むライセンス購入要求をライセンス管理サーバ 100 に送信し、ライセンス管理サーバ 100 からライセンス 110 を受信する。通信路 N を通じて、ライセンス管理サーバ 100 と端末装置 600 との間でライセンス 110 を送受信する場合には、セキュリティを確保するため、SAC を確立してから、データの送受信を行う。端末装置 600 は、受信したライセンス 110 を端末装置 600 に格納する。尚、本実施の形態では、ライセンス管理サーバ 100 と端末装置 600 との間で SAC を確立してからライセンス 110 を送受信するが、端末装置 600 に固有鍵が格納されており、ライセンス管理サーバ 100 が各端末装置 600 の固有鍵を管理している場合には、ライセンス 110 を端末装置 600 の固有鍵で暗号化してライセンス管理サーバ 100 から端末装置 600 に送信するなどしてもよい。

【0068】

(メタデータ受信 S1020)

次に、メタデータ 410 の受信処理について説明する。

端末装置 600 は、メタデータプロバイダ 400 に、メタデータ選択要求を送信し、メタデータ選択画面を受信する。端末装置 600 は受信したメタデータ選択画面を表示し、ユーザの操作により選択されたメタデータ 410 のメタデータ ID を含むメタデータ取得要求をメタデータプロバイダ 400 に送信し、メタデータプロバイダ 400 からメタデータ 410 を受信する。

【0069】

(公開鍵証明書受信)

次に、公開鍵証明書 510 の受信処理について説明する。

端末装置 600 は、コンテンツプロバイダ 300 に、公開鍵証明書要求を送信し、コンテンツプロバイダ 300 の公開鍵証明書 510 を受信する。

端末装置 600 は、メタデータプロバイダ 400 に、公開鍵証明書要求を送信し、メタデータプロバイダ 400 の公開鍵証明書 510 を受信する。

端末装置 600 は、CA 500 に、公開鍵証明書要求を送信し、CA 500 の公開鍵証明書 510 を受信する。

【0070】

(メタデータとコンテンツ利用 S1040)

次にコンテンツプロバイダ 300 またはメタデータプロバイダ 400 が署名したメタデータの利用可否判定について図 8 を用いて説明する。

メタデータ 410 がユーザ作成メタデータであるか否かを判定する (ステップ S200)。ユーザ作成メタデータ判定 (ステップ S200) の処理については後述する。ユーザ作成メタデータでない場合は署名者識別情報判定 (ステップ S100) に遷移し、ユーザ作成メタデータの場合 (後述する値「0」の場合) はステップ S201 に遷移する。

署名者識別情報判定 (ステップ S100) では、ライセンス 110 の利用条件 114 から署名者識別情報を取得し、“コンテンツプロバイダ以外不可” または “コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能” または “全て可能” のいずれであるかを判定する。

【0071】

署名者識別情報が “コンテンツプロバイダ以外不可” または “コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能” の場合には、ID 比較 (ステップ S101) に遷移する。

署名者識別情報が“全て可能”の場合にはCRL確認（ステップS110）に遷移する。

【0072】

ID比較（ステップS101）について図11を用いて説明する。

ID比較（ステップS101）では、暗号化コンテンツ310をコンテンツ暗号鍵115で復号してコンテンツプロバイダID312を取得し、メタデータ410からメタデータ署名者ID412を取得し、比較する（ステップS301）。コンテンツプロバイダID312とメタデータ署名者ID412が一致する場合は署名検証（ステップS102）に遷移する。コンテンツプロバイダID312とメタデータ署名者ID412が一致しない場合は、署名者識別情報を確認する（ステップS302）。

【0073】

署名者識別情報が“コンテンツプロバイダ以外不可”の場合は、署名者識別情報で利用可能なメタデータの署名者が“コンテンツプロバイダ以外不可”と設定されているのに、メタデータ410の署名者がコンテンツプロバイダ300以外であるため、メタデータ410は利用不可である。

署名者識別情報が“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”の場合は、メタデータ署名者ID412と主体者ID511が一致する公開鍵証明書510の証明書署名者ID514とコンテンツプロバイダID312とを比較する（ステップS303）。証明書署名者ID514とコンテンツプロバイダID312とが一致する場合は、署名検証（ステップS102）に遷移する。証明書署名者ID514とコンテンツプロバイダID312が一致しない場合は、署名者識別情報で利用可能なメタデータの署名者が“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”と設定されているのに、メタデータの署名者がコンテンツプロバイダ300およびコンテンツプロバイダ300に委任されたメタデータプロバイダ400以外であるため、メタデータ410は利用不可である。

【0074】

署名検証（ステップS102）では、メタデータのデジタル署名のメタデータ署名者ID412と一致する主体者ID511を含む公開鍵証明書510を取得し、公開鍵証明書510に含まれる主体者公開鍵512を用いてメタデータのデジタル署名を復号し、メタデータ本体411とメタデータ署名者ID412のハッシュ値と比較し、一致する場合はメタデータ410が利用可能と判定し、一致しない場合は改ざんされているために利用不可と判定する。

【0075】

CRL確認（ステップS110）では、メタデータ410のメタデータ署名者ID412がCRL520のリボークされた主体者ID522に含まれているか判定し、含まれていない場合には、署名検証（ステップS102）に遷移し、含まれている場合には、署名者がリボークされているためにメタデータ410は利用不可と判定する。

以上の処理により、ライセンス110の利用条件114に格納されている署名者識別情報に基づきメタデータの利用可否を判定することが可能となる。

【0076】

尚、本実施の形態では、署名者識別情報を“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”の3つの値から1つの値を識別するフラグとしたが、“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”のうちの少なくとも2つの値から1つの値を識別するフラグとしてもよい。この場合、例えば、署名者識別情報が“コンテンツプロバイダ以外不可”または“全て可能”を識別するフラグであれば、本実施の形態における署名者識別情報が“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”である場合の処理が行われなくなり、署名者識別情報が“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテ

ツプロバイダに委任されたメタデータプロバイダ可能”を識別するフラグであれば、本実施の形態における署名者識別情報が“全て可能”である場合の処理が行われなくなるが同様の効果をもたらす。

【0077】

尚、本実施の形態では、署名者識別情報判定（ステップS100）で署名者識別情報が、“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”の場合にCRL確認（ステップS110）を行わないが、署名者識別情報判定（ステップS100）以降に行ってもよい。

尚、本実施の形態では、コンテンツライセンス110の利用条件114に署名者識別情報が格納されているが、コンテンツライセンス110の中の利用条件114以外に格納されていてもよい。また、署名者識別情報が暗号化コンテンツ310に格納されていてもよい。また、コンテンツと同様にメタデータが暗号化され、暗号鍵を含むメタデータ410のライセンスがある場合、署名者識別情報がメタデータ410のライセンスに格納されていてもよい。以上の場合、署名者識別情報の取得先が異なるが同様の効果をもたらす。

尚、本実施の形態では、署名者識別情報を“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”を示すフラグとしたが、メタデータ410のメタデータ署名者ID412としてもよい。この場合、利用可能なメタデータの署名者がメタデータ署名者ID412の署名者に限定されるが同様の効果をもたらす。

【0078】

尚、本実施の形態では、メタデータ410のメタデータ署名者ID412がコンテンツプロバイダIDであるか否かのID比較（ステップS101）に、暗号化コンテンツ310に含まれているコンテンツプロバイダID312を用いているが、端末装置600に出荷時などあらかじめコンテンツプロバイダの公開鍵証明書510のみが格納されている場合には、公開鍵証明書510に含まれている主体者ID511を用いてもよい。また、端末装置600に出荷時などにあらかじめコンテンツプロバイダIDのみが格納されている場合には、格納されているコンテンツプロバイダIDを用いてもよい。また、メタデータ410のライセンスがあり、メタデータ410のライセンスにコンテンツプロバイダIDが格納されている場合、メタデータ410のライセンスのコンテンツプロバイダIDを用いてもよい。以上のいずれの場合でも、コンテンツプロバイダ300のコンテンツプロバイダIDが特定できるため同様の効果をもたらす。

【0079】

次に、ユーザによるメタデータの作成処理について説明する。

ユーザの入力操作に従い、端末装置600は、メタデータを作成する。具体的には、ユーザ作成メタデータであることを示すユーザ作成フラグと、シーンインデックスなどの情報とをメタデータ本体411に格納し、メタデータ作成者がユーザであることを示すために、メタデータ署名者ID412に値0を格納し、デジタル署名413にデジタル署名せずに値0を格納する。

【0080】

尚、本実施の形態では、メタデータ署名者ID412とデジタル署名413に値0を格納する場合について記述するが、ユーザにより端末装置600で作成されたメタデータ410を識別できれば他の値でもよい。

尚、本実施の形態では、ユーザ作成メタデータにデジタル署名しないが、全端末装置600がメタデータ署名者ID412と、秘密鍵と、公開鍵証明書510を保有している場合には、デジタル署名してもよい。この場合、後述するユーザ作成メタ判定（ステップS200）では、メタデータ410のデジタル署名者がユーザの所有する端末装置600であるか否かの判定を行う。

【0081】

端末装置600は、ライセンス110の利用条件114からユーザ作成メタデータの移

動範囲指定情報を取得し、“移動無制限”であれば、上記処理で作成したメタデータをそのまま端末装置 6 0 0 などに蓄積し、“メタデータを作成したユーザが所有する端末装置に限定”であれば、メタデータ本体 4 1 1 をドメイン鍵 2 1 2 で暗号化して端末装置 6 0 0 や DVD-R などの外部記憶媒体などに蓄積するか、ユーザが所有する他の端末装置 6 0 0 に送信する。この場合、メタデータ本体 4 1 1 がドメイン鍵で暗号化されているため、異なるドメインの端末装置 6 0 0 がメタデータ 4 1 0 を取得しても利用できない。

【0082】

尚、本実施の形態では、ユーザ作成メタデータの移動範囲指定情報が“メタデータを作成したユーザが所有する端末装置に限定”の場合にドメイン鍵 2 1 2 を用いてメタデータ本体 2 1 2 を暗号化しているが、ユーザが所有する端末装置 6 0 0 に共通の秘密情報であれば他の情報を用いてもよい。

【0083】

次にユーザが作成したメタデータの利用可否判定について図 9 を用いて説明する。

端末装置 6 0 0 は、ユーザ作成メタ判定（ステップ S 2 0 0）を行う。

ユーザ作成メタ判定（ステップ S 2 0 0）では、メタデータ 4 1 0 のメタデータ署名者 ID 4 1 2 が値 0 であるか判定する。値 0 でない場合は署名者識別情報判定（ステップ S 1 0 0）に遷移し、値 0 の場合はユーザ作成メタ利用可否判定（ステップ S 2 0 1）に遷移する。

【0084】

ユーザ作成メタ利用可否判定（ステップ S 2 0 1）では、ライセンス 1 1 0 の利用条件 1 1 4 からユーザ作成メタデータによる制御可否情報を取得し、“ユーザ作成メタデータによる制御不可”であれば、メタデータ 4 1 0 は利用不可である。ユーザ作成メタデータによる制御可否情報が“ユーザ作成メタデータによる制御可能”の場合には、ユーザ作成メタデータ移動範囲判定（ステップ S 2 0 2）に遷移する。

【0085】

ユーザ作成メタデータ移動範囲判定（ステップ S 2 0 2）では、ライセンス 1 1 0 の利用条件 1 1 4 からユーザ作成メタデータの移動範囲指定情報を取得し、“移動無制限”であれば、上記処理で作成したメタデータ 4 1 0 は利用可能と判定する。ユーザ作成メタデータの移動範囲指定情報が“メタデータを作成したユーザが所有する端末装置に限定”であれば、メタデータ本体 4 1 1 をドメイン鍵 2 1 2 で復号し、ユーザ作成メタデータであることを示すユーザ作成フラグがあるか否か判定する（ステップ S 2 0 3）。ユーザ作成フラグがない場合には、メタデータ 4 1 0 は利用不可である。ユーザ作成フラグがある場合には、メタデータ 4 1 0 は利用可能と判定する。

【0086】

尚、本実施の形態では、移動範囲指定情報を、“ユーザ作成メタデータによる制御可能”または“ユーザ作成メタデータによる制御不可”のいずれかを示すフラグとし、移動範囲指定情報が“ユーザ作成メタデータによる制御可能”の場合には、ドメイン鍵 2 1 2 を用いてユーザ作成メタデータを暗号化することで、ユーザ作成メタデータの移動範囲をユーザの所有する端末装置 6 0 0 間に限定しているが、移動範囲指定情報として移動回数や移動有効期間などの利用条件を格納し、端末装置 6 0 0 で生成した暗号鍵でユーザ作成メタデータを暗号化し、暗号鍵を含むユーザ作成メタデータのライセンスに移動範囲指定情報として格納された移動回数や移動有効期間などの利用条件を設定することで、移動を制限することにしてもよい。この場合、ユーザ作成メタデータの移動範囲は、移動範囲指定情報として格納された移動回数や移動有効期間などにより制限される。

【0087】

以降に、上記の判定処理でメタデータ 4 1 0 が利用可能と判定した後で行う処理について説明する。

まず、メタデータ参照必須コンテンツの利用処理について説明する。

端末装置 6 0 0 は、ライセンス 1 1 0 の利用条件 1 1 4 からメタデータの参照指示情報があるか否か検索し、参照指示情報がない場合は、暗号化コンテンツ 3 1 0 の利用を開始

する。参照指示情報がある場合は参照指示情報を取得し、参照指示情報に含まれるメタデータIDから参照すべきメタデータを取得し、メタデータの利用可否判定で利用可能な場合にメタデータを参照してコンテンツの利用を開始する。参照すべきメタデータが取得できない場合と、メタデータの利用可否判定で利用不可の場合にはコンテンツの利用ができない。

【0088】

尚、本実施の形態では、参照指示情報をメタデータIDとしたが、メタデータ署名者ID412でもよい。

尚、本実施の形態では、参照指示情報をメタデータIDとしたが、例えば、暗号化コンテンツ310とメタデータ410が共に端末装置600に送信されるなどして、暗号化コンテンツ310とメタデータ410が関連付けられている場合には、参照指示情報は、参照するか参照しないかを識別するフラグでもよい。

【0089】

次にユーザによるメタデータの編集処理について説明する。

端末装置600は、ライセンス110の利用条件114からメタデータの編集可否情報を取得し、“メタデータ編集可能”または“メタデータ編集不可”のいずれかを判定する。メタデータの編集可否情報が“メタデータ編集不可”の場合は、暗号化コンテンツ310のコンテンツID311をメタデータ本体411に含むメタデータ410は編集不可である。メタデータの編集可否情報が“メタデータ編集可能”の場合は、ユーザ操作に従い、暗号化コンテンツ310のコンテンツID311をメタデータ本体411に含むメタデータ410を編集し、編集したメタデータ410を含む再デジタル署名要求を、メタデータ署名者ID412の署名者に送信し、メタデータ署名者ID412の署名者が再デジタル署名したメタデータ410を受信する。

【0090】

尚、本実施の形態では、編集可否情報が“メタデータ編集可能”または“メタデータ編集不可”のいずれかを示すフラグであるが、編集可能なメタデータ410のメタデータIDであってもよい。この場合、編集可否情報で指定されたメタデータ410のみが編集可能と判定される。

同様に編集不可なメタデータ410のメタデータIDであってもよい。この場合、編集可否情報で指定されたメタデータ410のみが編集不可と判定される。

【0091】

尚、本実施の形態では、メタデータ410を編集後にメタデータ署名者ID412の署名者により再デジタル署名しているが、端末装置600が公開鍵と、秘密鍵と、公開鍵証明書510を保有している場合、端末装置600がメタデータ410にデジタル署名してもよい。

【産業上の利用可能性】

【0092】

本発明に係るコンテンツ配信システム1は、コンテンツプロバイダ300によりメタデータ410の利用を制御できるため、コンテンツプロバイダ300が意図しない信頼性の低いメタデータを排除できるコンテンツ配信システムとして有用である。

【図面の簡単な説明】

【0093】

【図1】本発明の実施の形態に係るコンテンツ配信システム1の全体の概略構成を示す図である。

【図2】本発明の実施の形態に係るライセンス110の構成を示す図である。

【図3】本発明の実施の形態に係るユーザ情報DB201のテーブル構成を示す図である。

【図4】本発明の実施の形態に係る暗号化コンテンツ310の構成を示す図である。

【図5】本発明の実施の形態に係るメタデータ410の構成を示す図である。

【図6】本発明の実施の形態に係る公開鍵証明書510の構成を示す図である。

【図 7】本発明の実施の形態に係る CRL 520 の構成を示す図である。

【図 8】本発明の実施の形態に係るコンテンツプロバイダ 300 またはメタデータプロバイダ 400 が署名したメタデータの利用可否判定の処理を示すフローチャートである。

【図 9】本発明の実施の形態に係るユーザが作成したメタデータの利用可否判定の処理を示すフローチャートである。

【図 10】本発明のコンテンツ配信システムの概略処理を示すフローチャートである。

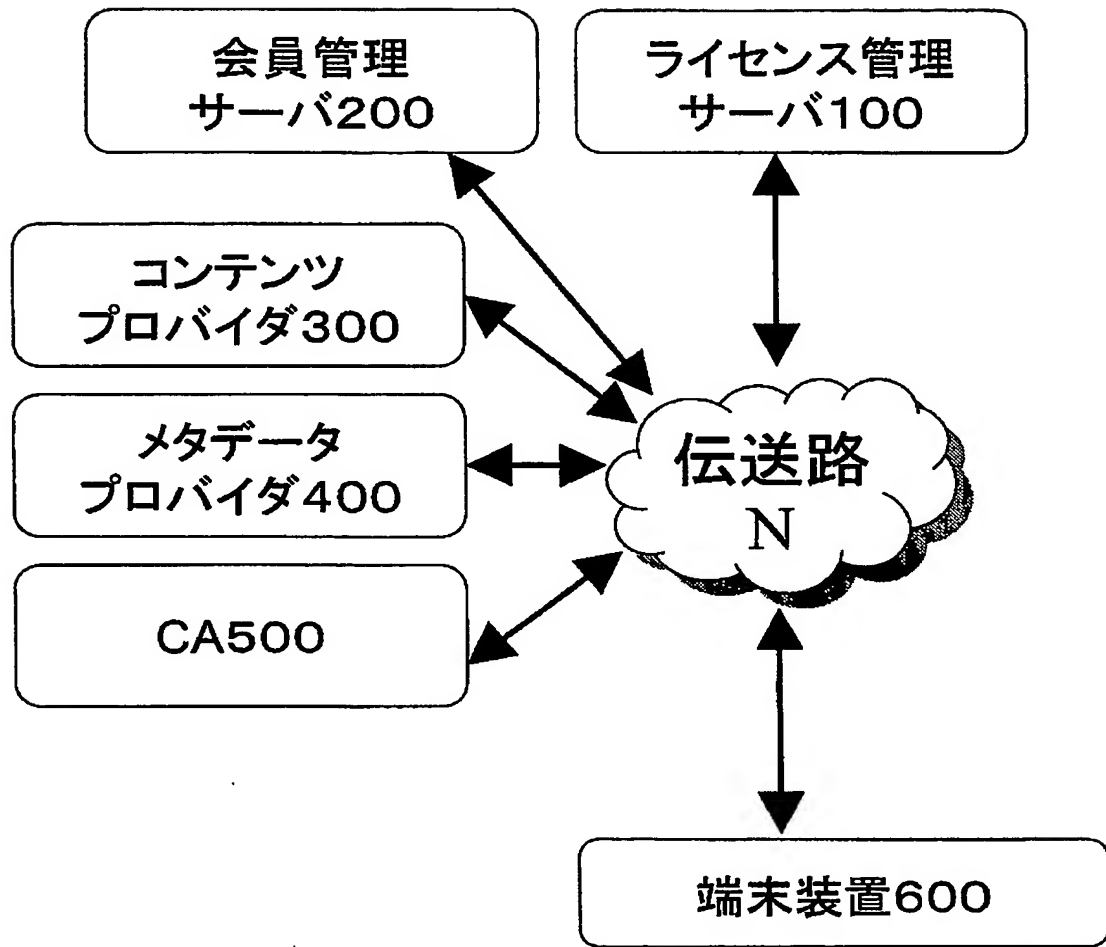
【図 11】図 8 に示される ID 比較 (ステップ S101) 処理の詳細を示すフローチャートである。

【符号の説明】

【0094】

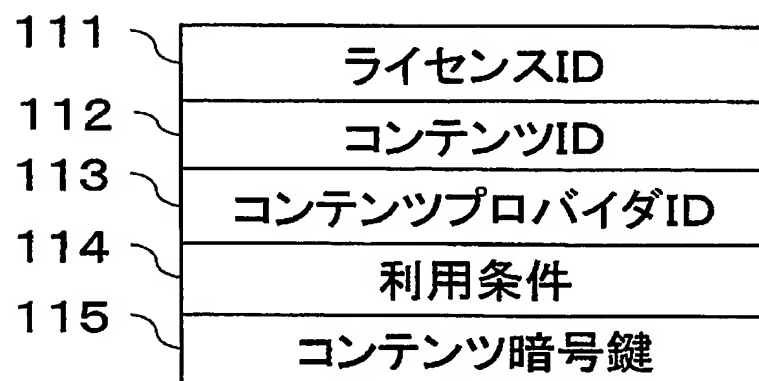
- 1 コンテンツ配信システム
- 100 ライセンス管理サーバ
- 200 会員管理サーバ
- 300 コンテンツプロバイダ
- 400 メタデータプロバイダ
- 500 CA
- 600 端末装置
- 110 ライセンス
- 111 ライセンス ID
- 112 コンテンツ ID
- 113 コンテンツプロバイダ ID
- 114 利用条件
- 115 コンテンツ暗号鍵
- 210 ユーザ情報 DB
- 211 ユーザ ID
- 212 ドメイン鍵
- 310 暗号化コンテンツ
- 311 コンテンツ ID
- 312 コンテンツプロバイダ ID
- 313 コンテンツ本体
- 410 メタデータ
- 411 メタデータ本体
- 412 署名者 ID
- 413 デジタル署名
- 510 公開鍵証明書
- 511 主体者 ID
- 512 主体者公開鍵
- 513 デジタル署名
- 514 署名者 ID
- 520 CRL
- 521 更新日時
- 522 リボークされた主体者 ID

【書類名】 図面
【図 1】



コンテンツ配信システム 1

【図 2】



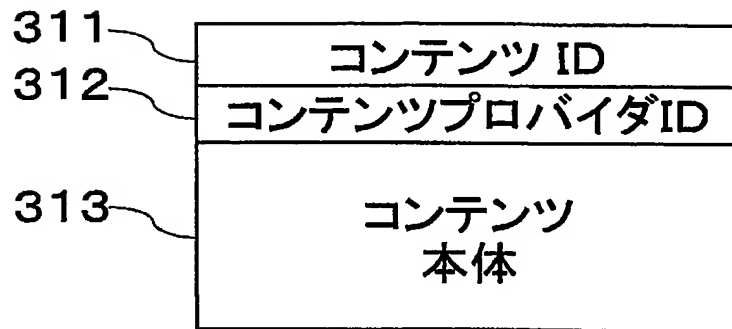
ライセンス 110

【図 3】

211 ユーザID	212 ドメイン鍵
XXXAAA	XXXCCC
XXXBBB	XXXDDD
.	.

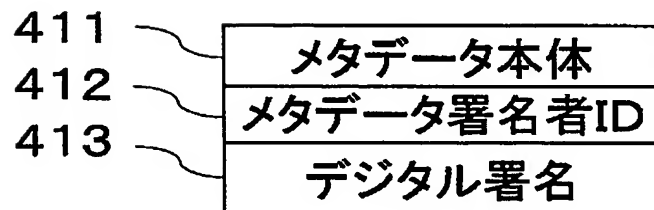
ユーザ情報DB 210

【図 4】



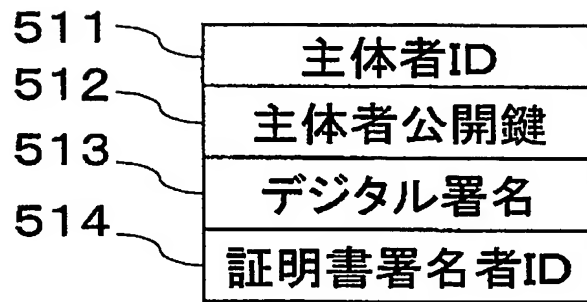
暗号化コンテンツ 310

【図 5】



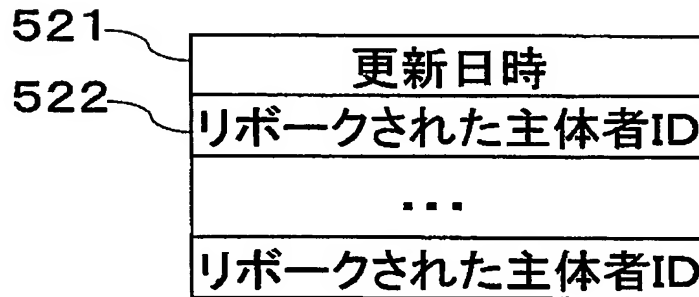
メタデータ 410

【図 6】



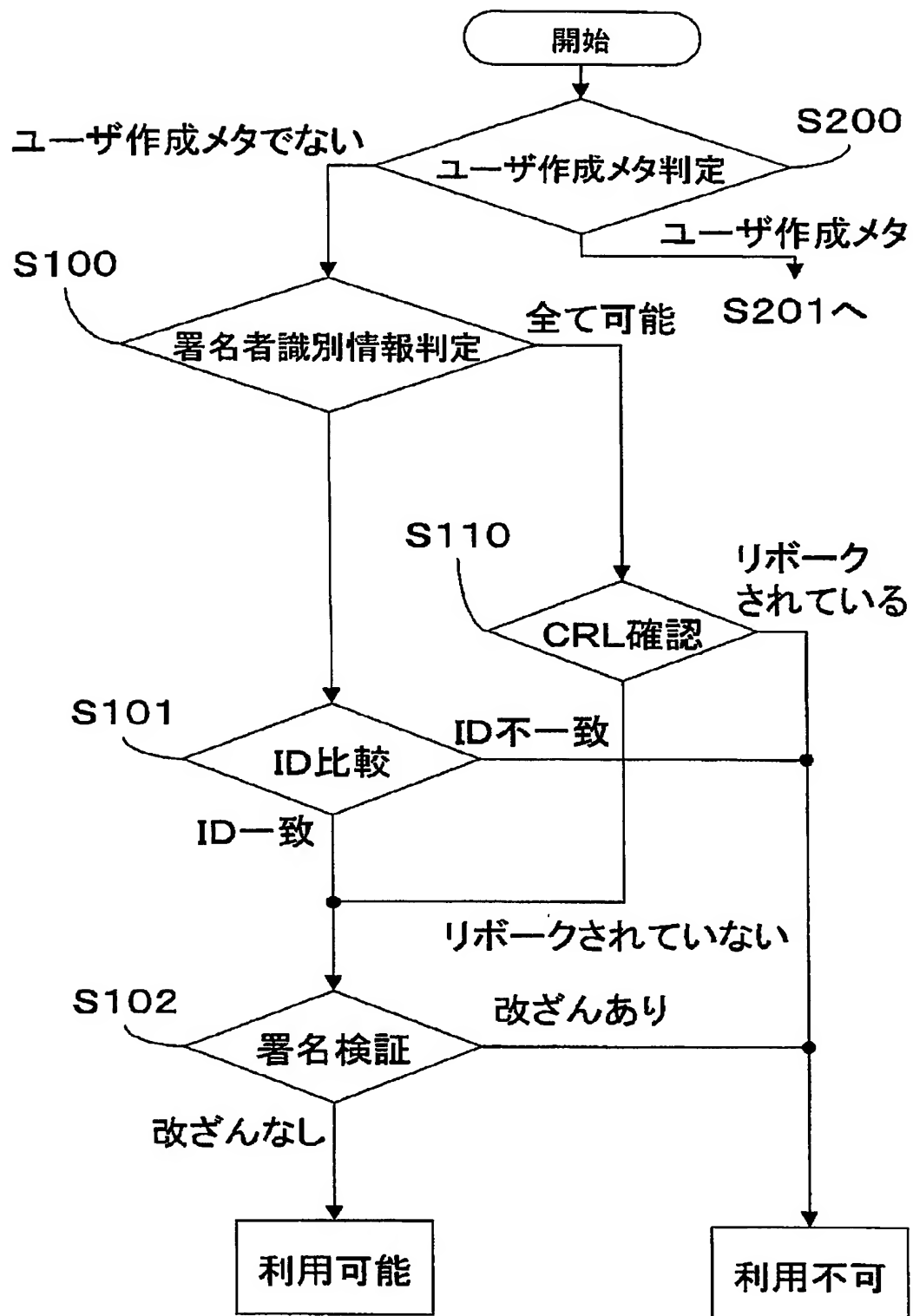
公開鍵証明書 510

【図 7】

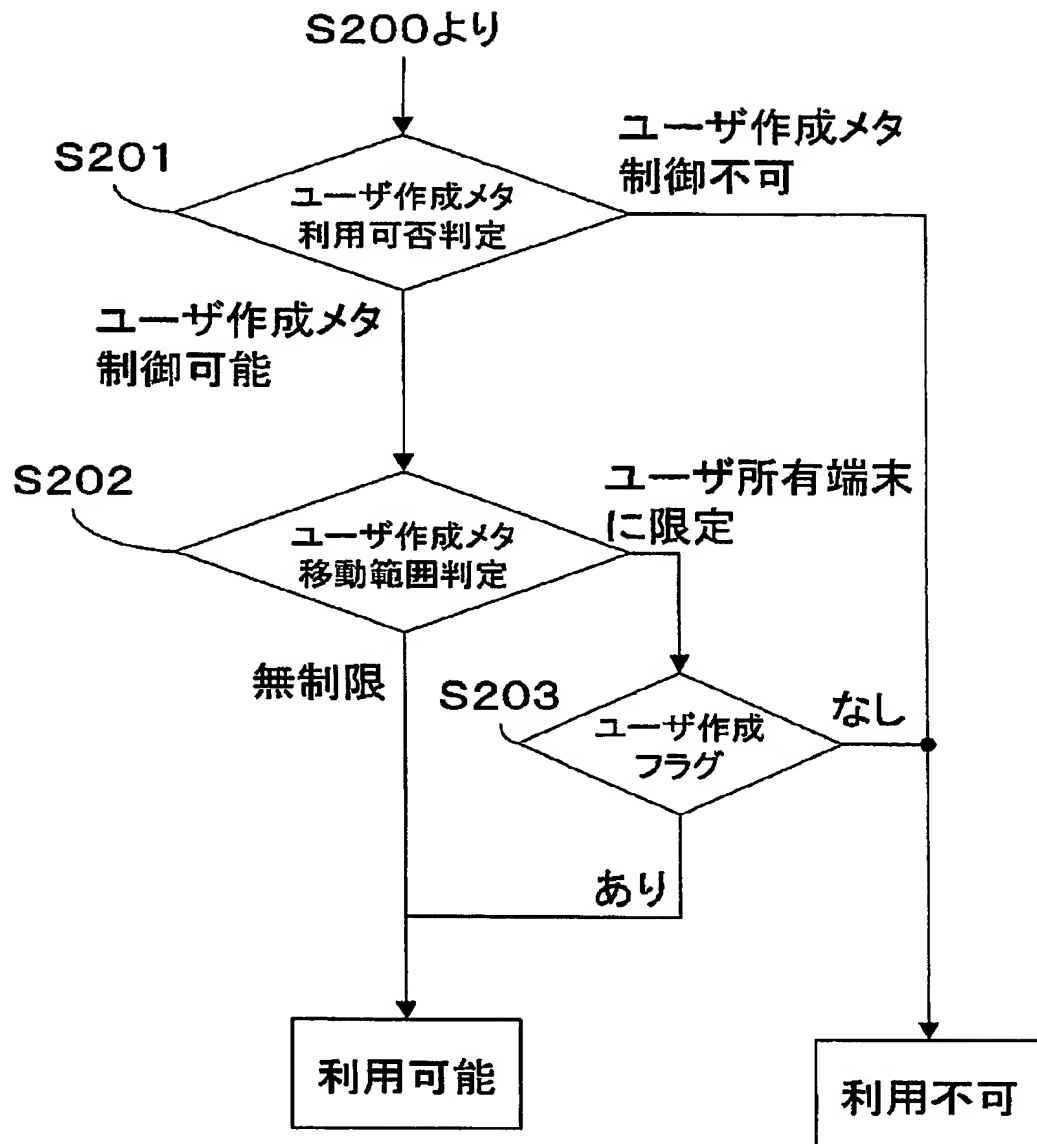


CRL 520

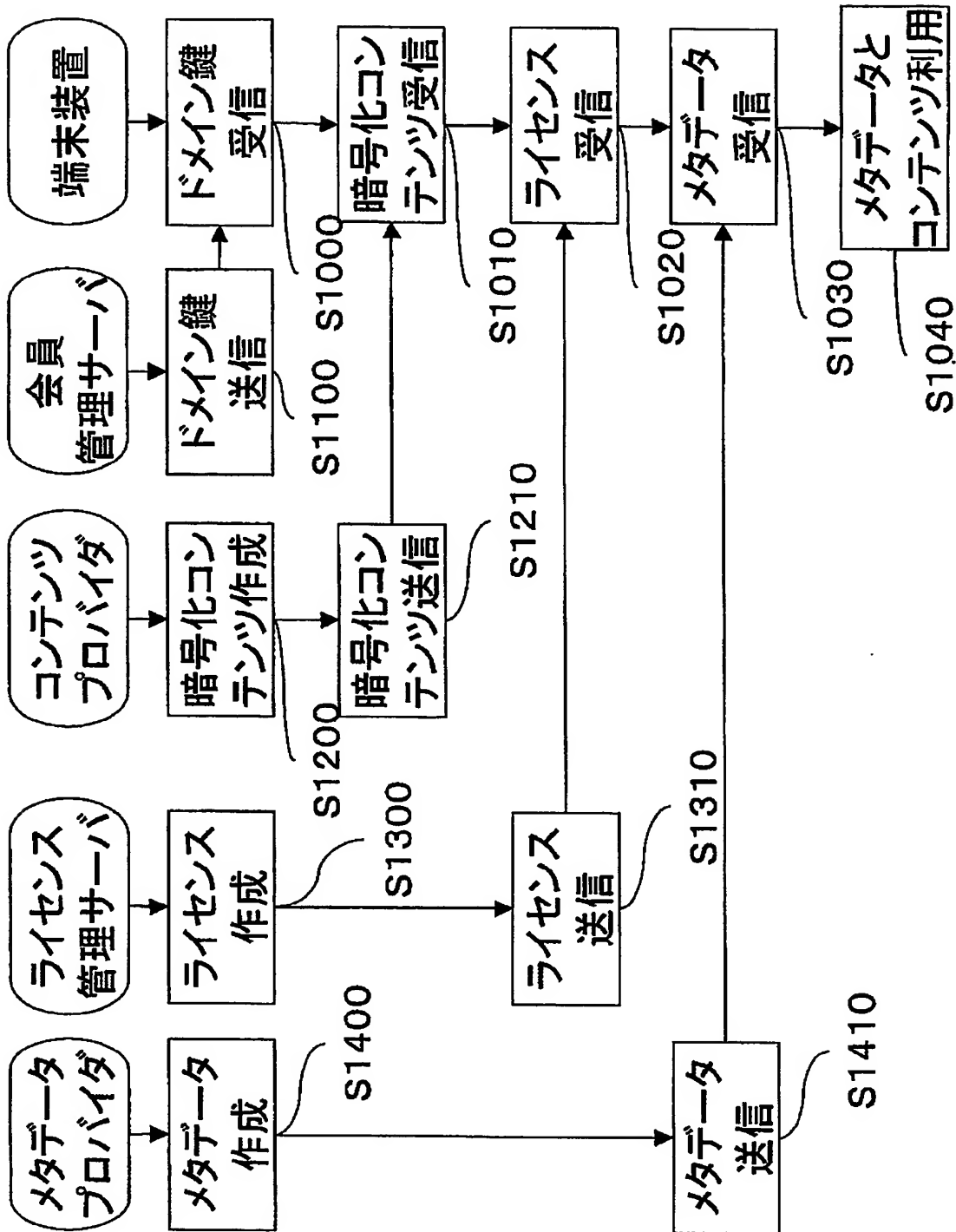
【図 8】



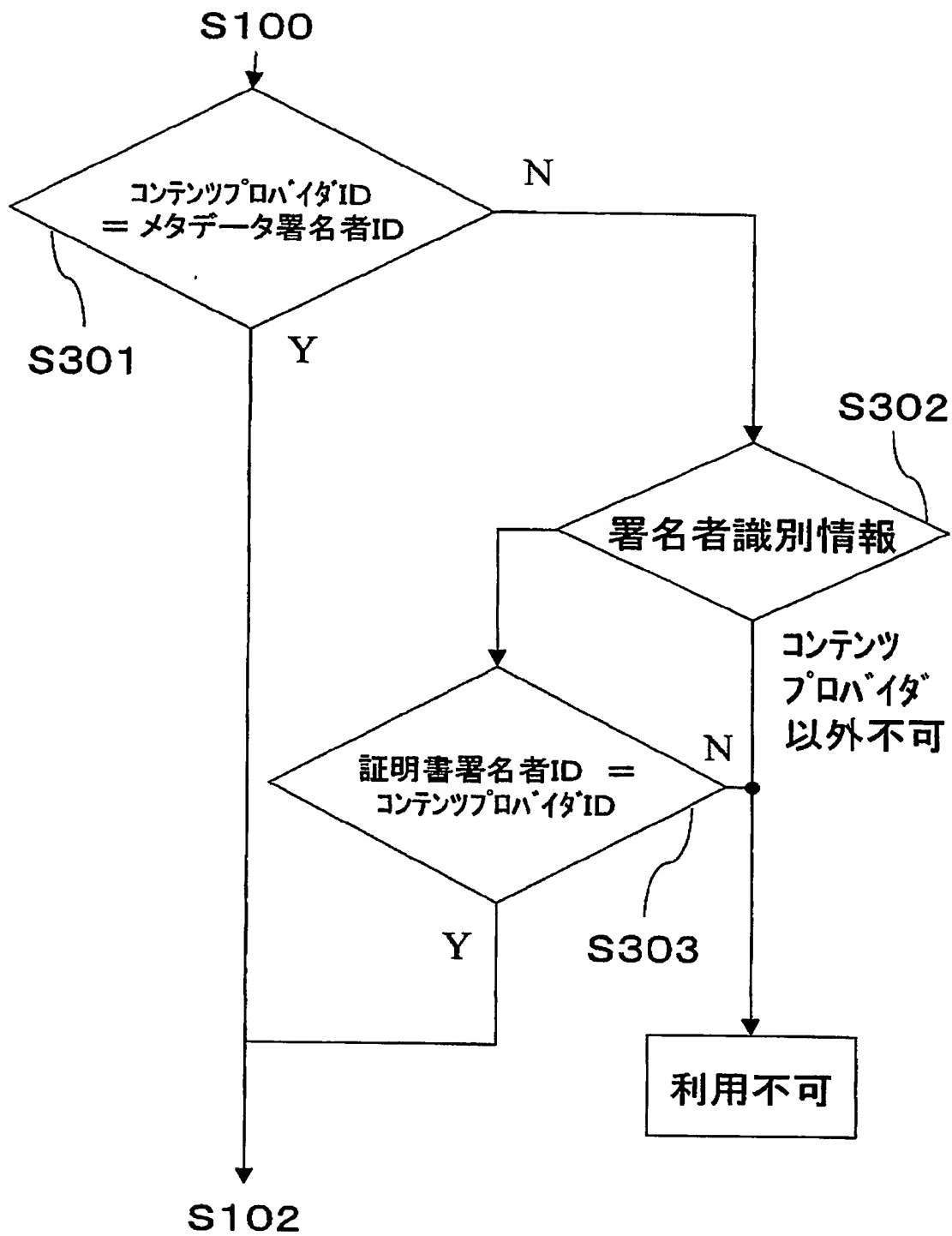
【図 9】



【図 10】



【図 11】



【書類名】要約書

【要約】

【課題】 コンテンツの提供者がデジタル署名したメタデータのみ利用可能なコンテンツ配信システムを提供する。

【解決手段】 端末装置 6 0 0 は、署名者識別情報判定（ステップ S 1 0 0）で、ライセンス 1 1 0 の利用条件 1 1 4 から取得した署名者識別情報が “コンテンツプロバイダ以外不可” の場合に、暗号化コンテンツ 3 1 0 から取得したコンテンツプロバイダ ID 3 1 2 とメタデータ 4 1 0 から取得したメタデータ署名者 ID 4 1 2 を ID 比較（ステップ S 1 0 1）し、一致しない場合はメタデータ 4 1 0 を利用不可とする。

【選択図】 図 8

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 3 8 0 8 4 9
受付番号	5 0 3 0 1 8 6 1 5 0 0
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 1 1 月 1 2 日

< 認定情報・付加情報 >

【提出日】	平成15年11月11日
-------	-------------

特願 2003-380849

ページ: 1/E

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住所

大阪府門真市大字門真1006番地

氏名

松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.